

HOW IT WORKS

Virtual private networks

A virtual private network helps you maintain fast, reliable communications wherever you are, but how does it work? Mike James explains how the internet gives remote users constant, secure access

A virtual private network (VPN) is an easy and cheap way to connect to your home or company network from anywhere in the world. It gives you access to all the facilities a local connection would bring. A VPN can even connect two distant private networks – for instance, two branch offices or two home networks – and make them behave like they are one network in one building.

The truly clever part is that you don't have to rent a secure, hardwired connection between the two; VPN offers an equivalent private connection on the cheap. A VPN uses the internet to make the connection. And if both ends of the connection already have broadband and one has Windows XP Professional Edition, you can set one up for free.

You'd be forgiven for wondering how safe it can be to pass private data across a public network inhabited by countless hackers and fraudsters. But you'll be a lot more confident about using a VPN once you know how it works.

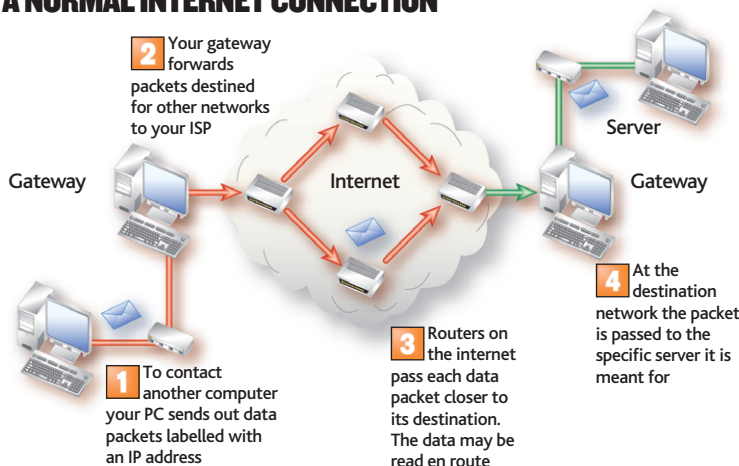
PACKETS WITHIN PACKETS

A VPN connection may pass through many PCs as it winds its way across the internet, but only the PCs at either end of the connection can get at the data transferred. This is very different to normal internet connections. Internet Protocol (IP) works by routing packets of data from source to destination. Every packet has a destination address; each time it reaches a router, the router works out where to pass it so it gets nearer to its destination. The route taken may involve many networks and vary from day to day; this is what makes the internet so flexible and robust. However, the data can be read as it passes through these networks, which makes the internet insecure.

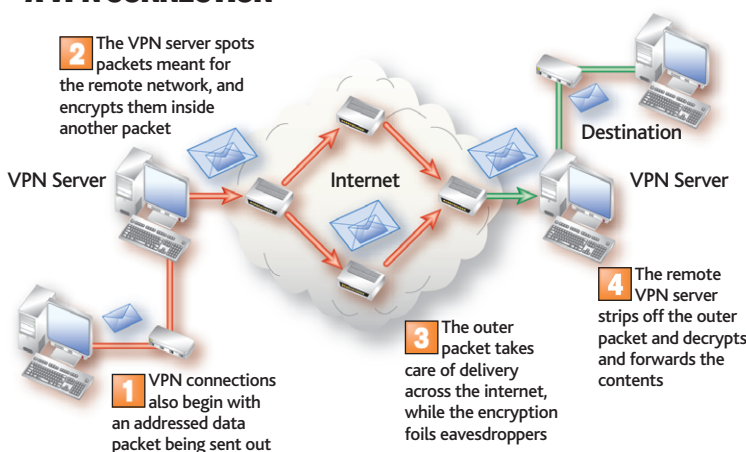
Local private networks use the same method of transferring data as the internet, but they keep the packets within your own building. Only when there is a need to exchange packets with the internet do they pass through a computer called a gateway and into the outside world.

The VPN gives you the best of both worlds, combining the free, long-distance data transport of the internet with the privacy of the local network.

A NORMAL INTERNET CONNECTION



A VPN CONNECTION



The site-to-site VPN involves two VPN servers. When a machine on private network A wants to send a packet to a machine on private network B, the packet is first sent to network A's VPN server. It is then encrypted and encapsulated within a standard IP packet that has a destination address corresponding to network B's VPN server. Both VPN servers have to be on the internet and have publicly accessible IP addresses. When the packet arrives at network B's VPN server, it extracts the encapsulated private packet, decrypts it and sends it on its way within the local network. As far as users of network A and B are concerned, the VPN is as good as a dedicated physical connection.

These two types of VPN use the same system of public data packets to transfer embedded and encrypted private data packets. This technique is called tunnelling, because it creates a private tunnel between two points that others cannot intercept.

IMPORTANT POINTS

Currently there are two main standards for these IP tunnels: Point-to-Point Tunnelling Protocol (PPTP) and Layer 2 Tunnelling Protocol/IP Security (L2TP/IPSec). These standards differ in the way the data is encapsulated. As we've said, using a VPN is a bit like dialling an ISP. So it should come as no surprise that PPTP and L2TP/IPSec

are based on the older Point-to-Point Protocol (PPP) used for dial-up internet access.

Microsoft, 3COM, US Robotics and others adapted PPP to produce PPTP. The main objection to PPTP is that it is proprietary. There have also been doubts about aspects of its security, although it has been improved in successive upgrades. Being a Microsoft-originated protocol, it is well supported on all versions of Windows from 98 onwards.

L2TP was drawn up by the Internet Engineering Task Force (IETF), the internet research body. For this reason, many regard it as better designed for the job and far more secure. L2TP uses IPSec for encryption purposes. This is a very flexible standard that should be capable of meeting most security requirements. However, L2TP/IPSec is supported only by Windows 2000, 2003 and XP clients.

They achieve this by taking private network packets, encrypting them and embedding them in public internet packets for delivery. This hiding of packets within packets is called encapsulation.

REMOTE POSSIBILITY

There are two types of VPN connection: the remote access VPN, where an off-site user dials into a network; and the site-to-site VPN, where two private networks are connected by a VPN link.

Using a remote access VPN to access a network feels like using an internet service provider (ISP) to access the internet. You connect to the VPN server and it checks your credentials and then gives you access to the network. All packets are encrypted and encapsulated before being transferred from your PC to the VPN server, or vice versa.



SECURITY MEASURES

This brings us to the most important aspect of any VPN protocol: security. VPN security has three components: authentication checks that the connection is being made by a legitimate user; access control determines which resources the authenticated user is allowed to access; and encryption encapsulates the data so it can only be accessed by both ends of the VPN connection.

Authentication and access control for users who connect via a VPN are similar to the security needed to control local users logging on to a network. There are additional issues, however, because the transaction occurs over the public internet rather than via the safety of a private network. For example, you may be happy with a password being sent across your private network without encryption, but if you sent it over the internet you don't know who might be eavesdropping. See our 'Who are you?' box (above right) for more details on how authentication works.

A more complex issue is the sort of encryption used to keep private data safe. PPTP uses Microsoft Point-to-Point Encryption (MPPE), which is a proprietary system, so it's more difficult for non-Windows machines to connect using PPTP. The MPPE encryption keys are derived from the password used to authenticate the connection. This keeps things simple as there is nothing to set up other than selecting a minimum key size; the actual key size is negotiated when the connection is made. However, the generated keys may be vulnerable to attack if the password they stem from is weak. Passwords containing repeated patterns mean keys can be cracked. But as long as strong passwords are used, MPPE is fine for most applications.

If you want the best security, you have to select L2TP when setting up your VPN. This takes a different approach to the problem of encryption. L2TP sets up IPsec encryption before it even authenticates the user. Almost the entire transaction between the client and server will appear scrambled to eavesdroppers. IPsec uses the Data Encryption Standard (DES) algorithm with a single 56-bit key, or three 56-bit keys for Triple DES (3DES), which was introduced after worries over the security of the standard DES algorithm.

IPsec also allows each data packet received to be authenticated to prove it was sent by the authorised client, and checked for integrity to prove it hasn't been tampered with. This is stronger security than that of PPTP, which ensures only that the data is difficult to read without the key.

KEY NOTES

IPsec is a general encryption and security protocol that can be used to secure any IP connection; a VPN is just one use of IPsec. IPsec doesn't use passwords to generate keys, as separate stronger keys are used. However, the keys do need to be distributed to both ends of the connection.

There are two ways of doing this. The first is to 'pre-share' keys. This just means that you type the same case-sensitive string of characters in to the client and the server. The pre-shared key is a simple idea, but how do you tell the remote user which key to type in without risking eavesdropping?

The other method involves digital certificates and public key cryptography. Public key cryptography uses an encoding scheme where a different key is required to encrypt and decrypt the

WHO ARE YOU? AUTHENTICATION ON A VPN

Authentication is a common problem. Proving who you are is usually just a matter of providing a username and a password. Things get more complicated when there's a chance that a third party might listen in on a connection – or even hijack it.

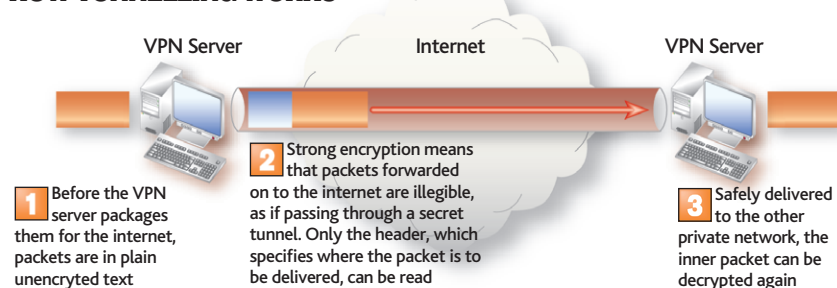
Both the common forms of VPN – PPTP and L2TP – offer the same range of authentication methods. The two most commonly encountered are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

PAP simply requests a username and password, and these are sent unencrypted. This just isn't secure. A better way involves Secure Password Authentication Protocol (SPAP), which encrypts the sensitive data. However the password is presented only once when the connection is made; this makes the connection vulnerable to hackers who might try to take it over.

CHAP is far better because it doesn't send any passwords between the client and the server. As both sides of a valid connection claim to know the password, either one can be challenged to compute a value based on it. The server sends a 'challenge', a code that can be combined with the password to produce a unique hash value. Both client and server compute this hash value, and the client sends theirs back to the server. If the client and the server have the same password, the hash values they both compute should match. If not, the server refuses access. The challenge-authenticate step can be repeated at any time. The client can even ask the server to authenticate in the same way.

There are different implementations of CHAP that don't necessarily work together; for example, MS-CHAP comes in a number of different versions, each more secure than the previous one.

HOW TUNNELLING WORKS



data. The encrypting key is made publicly available, while the matching decrypting key is kept private; it's impossible to calculate one from the other. The result is that anyone can send encrypted data, but only those with the private keys can decrypt and read data. As long as you guard the private keys carefully this system is completely secure, no matter which method you use to distribute the public keys. Such a system needs to be implemented on both ends of the VPN connection, which complicates matters, but it is worth doing.

SETTING UP A VPN

There are lots of guides to configuring a VPN on the internet (see the 'Further Information' box, right, for more information). The cheapest VPN to set up allows a single remote user to connect to a private network. This can be done using a standard copy of Windows XP Professional Edition as it includes a basic VPN server. More advanced server versions of Windows can connect lots of remote users at once. Windows 2000 and 2003 both offer VPN servers and there are free Windows VPN clients for all versions of Windows from Windows 98 onwards.

The remote user connects to the remote access server and from then on it's as if their local PC was part of the private network. This means that they can use file shares, pick up their email, browse the private website and do anything they could do if they were directly connected to the private network. In addition, they can use Windows' Remote Desktop feature to take control of a

machine on the private network and use it as if they were sitting in front of it.

As well as using Windows to implement a VPN, you can buy hardware that does the job. Some expensive routers incorporate a VPN server that you can connect to when away from the office or home. For further information, see the *Advanced Windows* article in our June 2005 issue, which explains the process of setting up a VPN using Windows XP Professional Edition and a hardware router. **ES**

FURTHER INFORMATION

The VPN Consortium
www.vpnc.org

Setting up Windows VPN clients and servers
www.onecomputerguy.com/networking.htm

Setting up a hardware router's VPN
www.homenethelp.com/vpn/router-config.asp

Microsoft VPN primer
www.microsoft.com/resources/documentation/windows/2003/all/techref/en-us/w2k3tr_vpn_what.asp

NEXT MONTH

BLU-RAY AND HD-DVD

The technological secrets of 30GB optical discs explored